

DataStarWeb

Documents

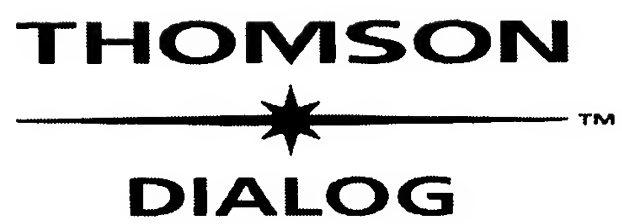


Table of Contents

INSPEC – 1969 to date (INZZ).....1

 Building certification paths: forward vs. reverse.....1

 Evaluating trust in a public key certification authority.....1

Search strategy.....3

Building certification paths: forward vs. reverse.

Accession number & update

7769766, C2003-12-1260C-005; 20031027.

Author(s)

Elley-Y; Anderson-A; Hanna-S; Mullan-S; Perlman-R; Proctor-S.

Author affiliation

Sun Microsystems Labs, Burlington, MA, USA.

Source

8th Annual Symposium on Network and Distributed System Security (NDSS'01), San Diego, CA, USA, 8-9 Feb. 2001.

In: p.8 pp., 2001.

Publication year

2001.

Language

EN.

Publication type

CPP Conference Paper.

Treatment codes

T Theoretical or Mathematical.

Abstract

In general, building and validating a certification path connecting a trust anchor to a target can be a very time-consuming process. As such, any optimizations are valuable. Certification paths are commonly built from the target to the trust anchor ("building in the forward direction") or from the trust anchor to the target ("building in the reverse direction"). This paper presents a comparison of these two approaches, analyzes the advantages and disadvantages of each approach, and concludes that building in the reverse direction is often more effective than building in the forward direction. (12 refs) .

Descriptors

certification; *public-key-cryptography*.

Keywords

certification path; trust anchor; reverse direction; forward direction; *public key* cryptography; signature; *public key certificate*.

Classification codes

C1260C (Cryptography theory).

C6130S (Data security).

Copyright statement

Copyright 2003, IEE.

COPYRIGHT BY Inst. of Electrical Engineers, Stevenage, UK

Evaluating trust in a *public key* certification authority.

USPTO Full Text Retrieval Options

Accession number & update

7111426, B2002-01-6120D-085, C2002-01-6130S-078; 20011203.

Author(s)

Chadwick-D-W; Basden-A.

Author affiliation

IS Inst, Salford Univ, UK.

Source

Computers–Security (UK), vol.20, no.7, p.592–611, 2001. , Published: Elsevier.

CODEN

CPSEDU.

ISSN

ISSN: 0167–4048, CCCC: 0167–4048/01/ (\$20.00).

Availability

SICI: 0167–4048(2001)20:7L:592:ETPC; 1–H.

Publication year

2001.

Language

EN.

Publication type

J Journal Paper.

Treatment codes

A Application; P Practical.

Abstract

With the growth of many different *public key* infrastructures on the Internet, relying parties have the difficult task of deciding whether the sender of digitally signed message is really who the *public key certificate* says they are. We have built an expert system that calculates the amount of trust, or trust quotient, that one can place in the name to *public key* binding in a *certificate*. The structure of the expert system is based on the CPS framework of Chokhani and Ford (RFC 2527), whilst the relative importance of the various factors that comprise the trust quotient, were determined by inter-viewing PKI experts from around the globe. This paper discusses the knowledge analysis strategy employed to collect this expert information and how we used it to develop the KBS. The analysis of the results of the interviews are also presented, and they can be summarised succinctly as "there are some factors concerning trust in a PKI which nearly all experts agree upon, and there are other factors in which there is very little agreement at all". The importance of identifying contextual factors when building a knowledge base is very important. In many cases, a disagreement between experts, as shown by a bimodal split in importance, was traced to differences in context and we show how this can be a source of new knowledge. (14 refs).

Descriptors

certification; expert–systems; Internet; knowledge–based–systems; *public–key–cryptography*.

Keywords

public key certification authority; Internet; digitally signed message; trust quotient; *public key* binding; CPS framework; PKI experts; knowledge analysis; expert system; RFC 2527; knowledge base; trust evaluation.

Classification codes

B6120D (Cryptography).
C6130S (Data security).
C1260C (Cryptography theory).
C6170 (Expert systems and other AI software and techniques).
C7210N (Information networks).

Copyright statement

Copyright 2001, IEE.

COPYRIGHT BY Inst. of Electrical Engineers, Stevenage, UK

Search strategy

No.	Database	Search term	Info added since	Results
1	INZZ	public ADJ key ADJ certificate	unrestricted	57
2	INZZ	limit set 1 YEAR = 2001		2

Saved: 01-Sep-2005, 18:07:49 CET
